



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/080,639	02/21/2002	Paul A. Cronic	2401CIP	9753

7590 01/23/2006

SAWYER LAW GROUP LLP
P.O. Box 51418
Palo Alto, CA 94303

EXAMINER

BAYAT, BRADLEY B

ART UNIT	PAPER NUMBER
----------	--------------

3621

DATE MAILED: 01/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/080,639	Applicant(s) CRONCE, PAUL A.	
	Examiner Bradley B. Bayat	Art Unit 3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 November 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Status of Claims

This communication is in response to remarks and amendment filed on November 3, 2005.

- Claims 1, 5, 7 and 13 have been amended.

Thus, claims 1-14 remain pending.

Response to Arguments

Applicant's arguments filed on November 3, 2005 have been fully considered but they are not persuasive.

Applicant has amended claims 1 and 7 to recite, "at least one of the second private and public keys is digitally signed by the first private key of the software publisher (response p. 8)." Claims 5 and 13 have been amended to correct "typographical errors." Id.

Applicant argues that the cited reference (Venkatesan et al., 6,898,706 B1) "fails to teach or suggest such a software licensing mechanism and instead teaches a content protection scheme that protects non-executable data." Id. at 10. Thereafter, applicant repeats in its entirety column 5, lines 21-57 in the summary section of the cited reference. Applicant's background of the invention acknowledges that protection of content and licensing of content for authorized use have been a problem and represent one of the objects of applicant's invention [0006-0011]. In fact, the cited reference highlights that such a distinction cannot be made in a DRM system, "since the DRM initiative holds significant promise as a mechanism that will sufficiently restrict illicit copying of Internet accessible software objects and hopefully, by doing so, assure a

Art Unit: 3621

sufficient financial return to publishers of those objects for their legitimate consumer access and use (column 3, lines 59-67).

Applicant further argues that the cited reference fails to disclose a “chaining of certificates (response p. 11).” On the contrary, Venkatesan discloses, “[a]t run time, the key manager, in turn, checks integrity of all other critical components of enforcer 600 using digital signatures of their expected vendors. To achieve this, O/S 454 can utilize an authenticated boot process to assure its own security and then establish necessary chains of trust among various components of the O/S and particularly throughout enforcer 600 and DRM system 456 (column 19, lines 25-56).”

Applicant contends that the cited reference refers to a “secret key” yet the claimed invention provides for a private key (response p. 11). As is well known in the cryptographic art and disclosed in the background of the reference, “[d]epending on the specific cipher used, this secret can be, e.g., a simple key known only to a sender and a recipient, or can be a **private key** of a public/private key pair (column 3, lines 37-48; emphasis added).” The cited reference discloses that a “secret value” that may represent a public/private pair key would be associated with the software certificate (see columns 5-8; figure 5 and associated text). Furthermore, the reference discloses that the publisher could readily extract the fingerprint in that object. By querying its user database, the publisher could learn the identity of the client PC, in terms of its computer ID, that the pirate used, in some fashion, to commit piracy.

The publisher could then instruct the WA to revoke a software certificate that held by this particular client PC for use of that particular key. If the WA is also a certifying authority (CA), then a usual client certificate can simply be revoked. In this case, the watermark key itself does

not need to be certified. For purposes of simplicity, we will assume throughout the remainder of the description, that these two authorities are the same (column 16, line 55-column 17, line 6).

Moreover, the enforcer, as indicated in block 1350, decrypts the downloaded object, O.sub.fe.sup.WM, using the symmetric encryption key (k.sup.e.sub.i) extracted from the license to yield the decrypted, fingerprinted and watermarked object, M (i.e., O.sub.f.sup.WM), which is then stored within unencrypted buffer 650.

In addition, the verifier 620, in turn, compares the VID value contained in header 1010 and the PID value specified in the license (these VID and PID values being "expected" values) to actual VID and PID values extracted from the watermark detected in the object to determine if identical matches exist between the actual and expected values of the PID, and between the actual and expected values of the VID. Most importantly, the verifier also checks if the license is signed by the publisher whose PID value was found in the detected watermark. To accomplish this, the verifier requires the publisher's certificate, cert (PK.sub.VID). The encrypted store delivers this certificate together with the license. If issue and expiration times are used for both watermark keys and the license, verifier 620 will also determine whether the license was issued later than the watermark key and expires before the watermark key (i.e., "issue/expiration time conditions").

If these matches occur, the license is properly signed and, when applicable, the issue/expiration time conditions are met, verifier 620 passes, as symbolized by line 623, the value of the rights vector V, also specified in the license, to the client O/S, as the protection state of this object, to control further access and use of object C.sub.i while that object resides in decrypted form (as object M) within unencrypted buffer 650. In particular, if the rights vector

Art Unit: 3621

illustratively contains three separate one-bit values (v.sub.1, v.sub.2 and v.sub.3), as shown in FIG. 6, these bits, based on their current states, may specify use of the object as follows: v.sub.1 =allow/disallow running; v.sub.2 =allow/disallow permanent storage; and v.sub.3 =allow/disallow manipulation. Hence, bit v.sub.1 would be applied to control a state of software switch 654 situated at an output of buffer 650.

In the case of active objects, this switch, once set, would effectively permit the object to be executed or not, i.e., effectively pass through line 653, via switch 654, to output lead 655. In the case of passive objects, this switch would either permit a media driver, which will be used in rendering that object through a media card, to either render that object or not, again symbolized by effectively passing that object through line 653, via switch 654 to output lead 655. Bit v.sub.2 would be applied, as symbolized by line 607, to ES 610 to specify whether the encrypted object (C.sub.i) can remain within this store, or is to purged from this store after the object, in decrypted form, has passed through unencrypted buffer 650 and has either been executed or rendered, as appropriate. In that regard, the value of the rights vector for a given object taken in conjunction with a current user request to access and/or use that object will, through object usage process 1400 (shown in FIG. 14).

Applicant also notes that a keyword search of the reference reveals that the reference fails to teach "a software toolset (response pp.12-13)." The claim merely recites implementing the authorization process in a software toolset. Applicant's disclosure states:

[0010] Accordingly, what is needed is a toolset to enable software developers or published to easily convert their unprotected software products, such as programs or software resources, including clip art or fonts, to "license-managed" software products. This toolset should use a similar secure licensing system to the one it generates for the license-managed software product. In other words, the toolset ideally should use the same mechanisms to provide licenses for its own use as it provides for use with the

Art Unit: 3621

developer/publisher product. This licensing system should establish a secure identity link from the end user all the way back to the toolset provider for the purpose of accurately identifying the individuals within the chain, such that the source of the hack can be traced back to either the software publisher or end user, to assist in the effort to stop the illegal activities. The present invention addresses all of these needs.

[0103] A process for delivery of a flexible and easy to use secure software license for controlling use of a software product has been described. This same process can also be used to license software tools that handle the required tasks of generating a license-managed software product for a software publisher/developer. This process will be described in conjunction with FIG. 11 and FIG. 12 below.

[0104] Referring now to FIG. 13, a flow diagram showing the entire chain from the creation of the toolset to the end user acquiring a license for a software product is shown. At the top of the diagram is the certificate authority 1301, who provides the service of issuing digital certificates. As described below, this may be a function provided by the toolset publisher 1302. Next is the toolset publisher 1302. Using various components 214, 1310, 1311, and 1312, a license-managed version of the toolset 1320 is produced, as described in detail below. This product is sold to the software publisher 1303, and interacts over path 1322 with the toolset license server 102a via the license request document 700 and license response document 900 described above, with one major addition. The request document 700 in this case includes a publisher certificate request, and the response document 900 contains the requested publisher certificate 502 issued by the CA 1301, along with the CA certificate 504. The toolset license server 102a must communicate with the CA 1301 over path 1321 to request that the publisher certificate be issued.

[0105] The software publisher 1303, using the license-managed toolset 1320, generates a configuration 1313 containing the newly created product public/private key set for his software product 220, signed using his private publisher key related to the publisher certificate 502 returned via communication path 1322. The toolset 1320 then uses built-in functions and resources, the configuration data 1313, the product, publisher, and CA certificates, and the software program 215 to create a license-managed software product 220. The certificates and keys from the configuration document 1313 are used in the publisher's license server 102b, serving the same function as the toolset license server 102a except server 102b does not receive certificate requests and does not provide CA-issued certificates, as described above for server 102a.

[0106] The resulting software product 220 is used by the end user, as described in detail in conjunction with FIG. 1 through FIG. 10 above, with the license request 700 and license response 900 being exchanged via path 1331. This results in the end user having licensed access to the software product. The details of the software publisher and user interaction have been described above in some detail. The CA 1301 to toolset publisher

Art Unit: 3621

1302 to software publisher 1303 interaction summarized above in conjunction with FIG. 13 is described in detail below, in conjunction with FIG. 11 and FIG. 12.

The cited reference describes such a process in a comprehensive and dynamic system of preventing compromise by unauthorized parties, protecting content from abuse and protecting publishers via certificate authorities from illicit acts and access (column 7, lines 27-column 8, line 56).

Accordingly, the rejection is maintained and made **FINAL**.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Venkatesan et al. (hereinafter Venkatesan), US 6,898,706 B1.

As per the following claims, Venkatesan discloses:

1 A method for deliver of a license-managed toolset for creating a license-managed software product, the method comprising the step of:

(a) providing an authorization process, the authorization process including the steps of:

(i) creating a first public and private key pair for a software publisher (fig 7, step 800),

(ii) creating a second public and private key pair for a software program, at least one of the second private and public keys is digitally signed by the first private key of the software publisher (fig 7, step 800),

Art Unit: 3621

(iii) creating an authorization program for the software program, and embedding a copy of the first and second public keys in the authorization program (fig 7, step 850),

(iv) combining the authorization program with a software program, such that when the software program is invoked on a computer, the authorization program obtains a license for the software program by (fig 7, publisher, authority and client):

(1) creating a license request (fig 8, 860 license request via link),

(2) encrypting the license request using the second public key (fig 8, 870 encrypts fingerprint),

(3) transmitting the encrypted license request to a key authority (fig 8, 340),

(4) receiving an encrypted license from the key authority, wherein the license includes license terms (fig 7, license download to each client), and

(5) decrypting the license using the first public key, such that the license terms are used to control use of the software program (fig 7, step 1300);

(b) implementing the authorization process in a software toolset that is provided by a toolset publisher, wherein when the authorization process is invoked in the software toolset, the toolset publisher is the publisher in the authorization process and the software toolset is the software program in the authorization process (fig 7, step 1400), and

(c) implementing the authorization process in a software product that is provided by a publisher of the software product using the software toolset, wherein when the authorization process is invoked in the software product, the publisher of the software product is the publisher in the authorization process and the software product is the software program in the authorization process, whereby both the software toolset and the software product use the same authorization

Art Unit: 3621

process to obtain respective licenses (figure 5, publisher-client authorization process).

2 The method of claim 1 further includes the step of transferring the first and second private keys to a key authority for receiving license requests and generating licenses (fig 8, watermarking authority 340).

3 The method of claim 1 further includes the step of including product and customer information within the license request and license documents (fig 11, CID, PID, steps 1115, 1122).

4 The method of claim 1 further includes the step of associating the license request with a financial transaction, and incorporating financial transaction information within the license (fig 11, step 1115 payment information 1122 license generation).

5 The method of claim 1 further includes the steps of: (a) assigning a publisher ID to the publisher, (b) embedding the publisher ID within the authorization program, (c) including the publisher ID within the license, and (d) comparing the embedded publisher ID with the publisher ID within the license to verify the publisher of the software program to be authorized has generated the license (fig 11, step 1122).

6 The method of claim 1 further including the steps of: (a) generating a machine fingerprint within the authorization process, (b) incorporating the machine fingerprint within the license request, (c) incorporating the machine fingerprint within the license terms, and (d) using by the

Art Unit: 3621

authorization program the machine fingerprint to prevent use of the software product on a different machine than the one which made the license request (fig 11, step 1122).

7 A method for deliver of a license-managed toolset for creating a license-managed software product, the method comprising the step of:

- (a) providing an authorization process, the authorization process including the steps of:
 - (i) creating a first public and private key pair for a software publisher, and creating a first certificate with the public key using a certificate authority (column 13, lines 18-34), (ii) creating a second public and private key pair for a software program, and creating a second certificate with the software publisher private key, at least one of the second private and public keys is digitally signed by the first private key of the software publisher (column 13, lines 25-34), (iii) creating an authorization program for the software program, and embedding a copy of the first and second certificates and second private key in the authorization program (column 13, 35-48), (iv) combining the authorization program with a software program, such that when the software program is invoked on a computer, the authorization program obtains a license for the software program by: (1) creating a formatted license request, (2) signing the formatted license request using the second public key, (3) transmitting the formatted signed license request to a key authority, (4) receiving an signed formatted license from the key authority, wherein the license includes license terms, and (5) validating the license using the first certificate, such that the license terms are used to control use of the software program (fig 7 and as detailed in the above rejection of claim 1);

Art Unit: 3621

(b) implementing the authorization process in the software toolset that is provided by a toolset publisher, wherein when the authorization process is invoked in the software toolset, the toolset publisher is the publisher in the authorization process and the software toolset is the software program in the authorization process (fig 7, 1400), and

(c) implementing the authorization process in the software product that is provided by a publisher of the software product using the software toolset, wherein when the authorization process is invoked in the software product, the publisher of the software product is the publisher in the authorization process and the software product is the software program in the authorization process, whereby both the software toolset and the software product use the same authorization process to obtain respective licenses (fig 5, publisher-client authorization process).

8 The method of claim 7 further includes the step of including product and customer information within the license request and license documents (see claim 3 above).

9 The method of claim 7 further includes the step of associating the license request with a financial transaction, and incorporating financial transaction information within the license (see claim 4 above).

10 The method of claim 7 further includes the step of formatting the license request and license using a proposed signed XML document format (column 11, lines 1-23, note that XML encoding may occur within HTML content; XML DTD describes a subset of HTML 4.0 for embedded use within other XML).

11 The method of claim 7 further includes the step of generating the first public and private key pair for the software product publisher during the authorization process for the toolset, using the steps of: (a) creating the first public and private key pair for the software publisher prior to using the authorization process for the toolset; (b) including the public key within the license request document in the form of a certificate request; (c) receiving the certificate within the license document, and (d) using the received certificate in conjunction with the private key as the first key pair in the authorization process for the software product (see process in fig 5 and as detailed above rejected claims).

12 The method of claim 7 further includes the step of transferring the first and second private keys and certificates to a key authority for receiving license requests and generating licenses (fig. 8, step 900 watermarking authority 340).

13 The method of claim 7 further includes the steps of: (a) assigning a publisher ID to the publisher, (b) including the publisher ID within the publisher certificate, included within the software product license, (c) embedding the publisher ID within the authorization program, (d) comparing the embedded publisher ID with the publisher ID within the certificate to verify the publisher of the software program to be authorized has generated the license (fig 11, steps 1115, 1122).

14 The method of claim 7 further including the steps of: (a) generating a machine fingerprint

Art Unit: 3621

within the authorization process, (b) incorporating the machine fingerprint within the license request, (c) incorporating the machine fingerprint within the license terms, and (d) using by the authorization program the machine fingerprint to prevent use of the software product on a different machine than the one which made the license request (fig 11, steps 1115, 1122).

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 3621

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- US Patent 6,611,812 B2 to Hurtado et al.
- US Patent 6,904,523 B2 to Bialick et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley B. Bayat whose telephone number is 571-272-6704. The examiner can normally be reached on Tuesday - Friday 8 a.m.-6:30 p.m. and by email: bradley.bayat@uspto.gov.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached regarding urgent matters at 571-272-6712.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit: 3621

Any response to this action should be mailed to:

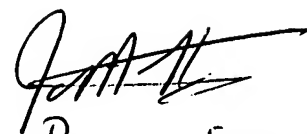
Commissioner of Patents and Trademarks
Washington, D.C. 20231

Or faxed to:

(571) 273-8300 - Official communications; including After Final responses.

(571) 273-6704 - Informal/Draft communications to the examiner.

bbb
January 13, 2006


Primary Examiner
AU 3621